REMARKS/ARGUMENTS

Claims 1-8 are pending. In this response, claims 1 and 6 have been amended. Thus, claims 1-8 will remain pending.

In the Office Action, the Examiner rejected all the claims over the cited references. In particular, the Examiner rejected claims 1-5 under 35 USC §102(e) as allegedly being anticipated by U.S. Patent No. 6,490,682 to Vanstone et al. (hereinafter "Vanstone") and rejected claims 6-8 under 35 USC §102(e) as allegedly being anticipated by U.S. Patent No. 6,467,684 to Fite et al. (hereinafter "Fite").

Claims 1-5

Claims 1-5 were rejected as allegedly being anticipated by Vanstone. In order to further the prosecution of the application, Applicants have amended claim 1 without acquiescence and prejudice, as set forth above. Applicants respectfully submit that amended claims 1-5 are not anticipated by Vanstone for reasons set forth below. A novel feature of the presently claimed invention lies in the speedup it achieves. It is known that it is preferred to process online transactions as rapidly as possible. Otherwise the customers will lose interest and go away and the merchant will lose business. This is one aspect that the presently claimed invention addresses. In particular, the presently claimed invention uses a single round-trip authentication scheme. This is not disclosed by Vanstone. Applicants respectfully submit that the Vanstone scheme employs at least two round-trips.

In addition to employing a single round-trip authentication scheme, the presently claimed invention provides several other elements that are also patentable over the Vanstone reference as recited by the claims depending from amended independent claim 1. These additional elements include: 1) the sequential generation of the challenge; 2) the challenge is a function of a running index and other information such as ID, time, etc.; 3) random generation of the challenge; and 4) the server sending the next challenge in advance. Furthermore, considering that dependent claims 2-5 include all of the features and elements of amended claim 1 from

which they depend, these claims are also patentable to the same extent that amended independent claim 1 is patentable.

Claims 6-8

Claims 6-8 were rejected as allegedly being anticipated by Fite. In order to further the prosecution of the application, Applicants have amended claim 6 without acquiescence and prejudice, as set forth above. Applicants respectfully submit that amended claims 6-8 are not anticipated by Vanstone for reasons set forth below.

Applicants do not disagree with the Examiner in that there are other known one-time credit card schemes in the literature. In fact, the Applicants refer to some of them in the background section of the specification of the present patent application, namely the Microsoft (paragraph 08) scheme and the Orbiscom (paragraph 15) scheme. Applicants respectfully note that two requirements for any such one-time credit card schemes are scalability and protection against frauds. The Fite scheme cited by the Examiner is very similar to the Microsoft scheme. In that scheme the number is generated at the client side and in the Orbiscom scheme, the number is generated by the issuer. Since many digits in the Microsoft one-time card number always remain the same (for the same customer), it is easy to make fraudulent attempts and succeed. That is, the fraud protection probability is low. On the other hand, in the Orbiscom scheme, since the one-time card number is generated by the issuer, it introduces an unwanted delay that may not be acceptable to the client.

The presently claimed invention overcomes these shortcomings of the Microsoft, Fite and Orbiscom schemes in a novel manner. The presently claimed scheme is highly scalable and at the same time has a very high fraud protection probability. What enables the presently claimed invention to overcome the shortcomings of the prior art is the generation of (most of the digits of) the one-time card number randomly. Since the one-time card number generated is random, it provides for a good protection against frauds. A merchant will have to try 10^{10} transactions, in the worst case, before being successful in one cheating (unauthorized and unauthenticated transaction). In addition, since the credit card number is very different from the

one-time number, the presently claimed scheme is enabled to support a large number of customers, or in other words, the presently claimed scheme is able to obtain superior scalability. Applicants have amended independent claim 6 as set forth above to better articulate and thus provide a suitable level of protection for the presently claimed invention. Applicants respectfully submit that amended claim 6 is not anticipated by the Fite reference for reasons set forth above.

In addition to employing a single round trip authentication scheme, and generating a one-time use card number at a user system using a random number generator, the presently claimed invention provides several other elements that are also patentable over the Fite reference as recited by the claims depending from amended independent claim 6. These additional elements include passing the one-time use card number to the issuer including passing at least one other data element related to the online transaction, and wherein the at least one other data element is selected from, or a function of, a user's account number, a user's private key, a transaction time, a transaction amount, or a merchant ID. Furthermore, considering that claims 7-8 derive patentability at least from their dependence on claim 5, these claims are also allowable, at least for the reasons set forth above for claim 6.

In summary, Applicants respectfully submit that the following features distinguish the presently claimed invention from the art cited by the Examiner. 1) the one time card generated in accordance with the embodiments of the present invention needs very simple software since it uses a random number generator for most of the digits; 2) the scalability and fraud protection in accordance with the embodiments of the present invention are superior to others'; and 3) more users can be supported by the presently claimed inventions, because in the prior art techniques only four digits are used as the customer ID, such that the usage of other schemes is very restricted. In stark contrast, the user of the method in accordance with the embodiments of the present invention generates a one-time card number and uses it with the merchant and at the same time sends this number and the permanent card number to the issuer. No such scheme is mentioned in any of the cited references.

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance and an action to that end is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 925-472-5000.

Respectfully submitted,

Babak Kusha
Reg. No. 51,095

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 925-472-5000
Fax: 415-576-0300
BK:lls
60291496 v1